A ZOOMRÓL REALISZTIKUSAN

A koronavírus-járvány elszabadulása elleni küzdelemben, a szabad mozgást korlátozó intézkedésekkel, a szociális távolságtartással, az otthoni munkavégzés általánossá válásával egyre nagyobb szerepet kapnak a videohívások lebonyolítását, konferenciabeszélgetéseket támogató szolgáltatások. Ennek a trendnek az egyik legnagyobb nyertese kétségkívül a felhő alapú vállalati kommunikációs platformot nyújtó Zoom, akiknél a meeting résztvevők száma márciusban elérte a napi kétszázmilliót.

A felhasználók fokozott érdeklődése mellett a szolgáltatás felkeltette a kiberbűnözők, az adatvédelmi aktivisták és a biztonsági szakemberek figyelmét is. Sorra jelennek meg legkülönbözőbb támadási formák, a feltárt sérülékenységek, adatvédelmi problémák, biztonsági elemzések. Világszerte akkora a szolgáltatás körüli érdeklődés, hogy az ember nem győzi kapkodni a fejét.

Összegyűjtöttünk a sajtóban megjelent, legnagyobb port felkavaró problémákat:

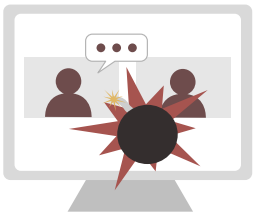
ADATHALÁSZAT, MEGTÉVESZTŐ URL-EK

A Zoom népszerűségének megugrásával menetrendszerűen megjelentek a Zoom-os linkekkel operáló adathalász támadások is, ugrásszerűen növekszik a Zooméhoz megtévesztően hasonló domainnevek regisztrációjának száma. Ezek ellen a konferenciabeszélgetés meghívónak álcázott támadások ellen sem lehet nagyon mást tenni, mint amit a biztonsági szakemberek mindig minden fórumon tanácsolnak:

- Ne kattintsunk gyanús, ismeretlen forrásból származó linkre, ne nyissunk meg ismeretlen feladótól kapott állományokat;
- Mindig ellenőrizzük a meghívóban szereplő linket, hogy tényleg a szolgáltató oldalára mutat-e, ha lehet ne a linken keresztül kapcsolódjunk a konferenciabeszélgetésbe, hanem a meeting ID közvetlen megadásával;
- Ha nem várt meghívót kapunk, vagy nem tudjuk egyértelműen azonosítani a szervező személyét ellenőrizzük független forrásból, kérdezzünk rá más csatornán, telefonon;
- Ellenőrizzük a szolgáltató oldalán a tanúsítvány érvényességét (van-e tanúsítvány, érvényes-e, tényleg a szolgáltatónak lett-e kiállítva, …);
- Ismeretlen, gyanús felületen ne adjunk meg azonosító, hitelesítő adatokat;
- Csak megbízható, ellenőrzött forrásból származó programot telepítsünk;
- Ne használjuk kiemelt jogosultsággal a gépünket.

Duna Tower , 1138 Budapest, Népfürdő u. 22.
t: +36 1 2704-835, f: +36 1 2704-329, e: info@kancellar.hu, w: kancellar.hu

HÍVÁS MEGZAVARÁSA, KÉRETLEN TARTALOM



Nagyon szembeötlő jelenség, támadási forma, hogy a hívatlan támadó becsatlakozik a konferenciabeszélgetésbe és kéretlen tartalmak megosztásával (tipikusan pornóval, hirdetésekkel) megzavarja azt. Ez ellen a legalapvetőbb védekezési módok a következők lehetnek:

- Ne osszuk meg nyilvánosan a konferenciabeszélgetés linkjét, azonosítóját, lehetőség szerint csak azoknak küldjük el akiknek tényleg számítunk a részvételére;
- A beszélgetéshez való csatlakozást kössük jelszó megadásához. Tovább növelhetjük a biztonságot, ha a jelszót nem a meghívóban küldjük ki a résztvevőknek, hanem külön csatornán (ne használjunk túl egyszerű, vagy könnyen kitalálható jelszót);
- Használjunk egyedi (egyszeri) azonosítókat ez eseményekhez;
- Használjuk a szolgáltató „várószoba" funkcióját így csak azok tudnak becsatlakozni a konferenciabeszélgetésbe, akiket explicit beengedünk;
- Konkrétan a Zoom esetében a szolgáltató az oldalán tájékoztatókat, ajánlásokat, oktatóvideókat, tesz közzé a szolgáltatás biztonságos használatával kapcsolatban, amikben a fentiek mellett számos hasznos funkciót bemutatnak, amelyek segítenek kontroll alatt tartani a konferenciabeszélgetést. Ezeket nézzük meg, válasszuk ki a nekünk még megfelelő, legbiztonságosabb funkciókat és használjuk azokat.

NYILVÁNOSSÁGRA KERÜLT SÉRÜLÉKENYSÉGEK

Az utóbbi időben több (egyébként igen aggasztó) sérülékenység került nyilvánosságra a Zoommal kapcsolatban. Az egyik ilyen miatt a támadók távolról be tudták kapcsolni a macOS-t használó áldozat mikrofonját és kameráját; egy másik sérülékenységet kihasználva a nem kellően biztonságos beállításokkal futó Windows munkaállomásokról lehet megszerezni a helyi felhasználó azonosítóját és jelszavát (a jelszó hash-t) a fájlok felcsatolásakor létrejövő linkek használatával; de olyan hiba is nyilvánosságra került, ami miatt az iOS program minden belépésnél adatokat küldött a felhasználókról a Facebooknak (függetlenül attól, hogy van-e FB accountjuk, vagy használják-e azt a Zoom bejelentkezéskor) és még számos más példát sorolhatnánk. Az eddig nyilvánosságra került sérülékenységek sajnos azt mutatják, hogy a rendszer fejlesztése/tervezése során nem kapott megfelelő hangsúlyt biztonságos fejlesztési szemlélet. Ezek alapján nem lenne meglepő, ha a közeljövőben még előkerülnének komoly biztonsági hiányosságok.

#StayAtHome

De hogy őszinték legyünk a szoftveripar sajnos már csak ilyen. Kivétel nélkül minden elterjedt videokonferencia platformban találtak már sérülékenységeket és feltehetően fognak is. A gyártók – és e tekintetben úgy tűnik a Zoom sem kivétel – folyamatosan dolgoznak a hibák kijavításán, folyamatosan adják ki a frissítéseket. Szerencsére a Zoom körüli fokozott érdeklődés a biztonsági szakemberek figyelmét is felkeltette, így sorban jelennek meg a biztonsági elemzések és remélhetőleg ezzel együtt folyamatosan javul a szolgáltatás biztonsági szintje. A Zoom a napokban jelentette be, hogy három hónapra befagyasztják az új funkciók fejlesztését és a fejlesztők csak a hibák javítására, a biztonsági szint növelésére fókuszálnak (jobb későn, mint soha).

E tekintetben akkor járunk el az elvárható gondossággal (mint bármilyen más szoftvertermék esetében), ha nyomon követjük a nyilvánosságra került sérülékenységeket, feltelepítjük a megjelenő biztonsági frissítéseket, illetve a legfrissebb klienst használjuk. Ha tudunk olyan funkcióról, aminek van ismert sérülékenysége, de még nem jelent meg hozzá a javítás, akkor azt nem használjuk. Emellett általában is javasolt, hogy csak azokat a funkciókat használjuk, amikre tényleg szükség van, pl. ne használjuk a videokonferencia szolgáltatást fájlok megosztására, különösen, ha az adott feladatra van más megbízhatóbb, vagy jobban a felügyeletünk alatt álló megoldás.

ADATVÉDELMI KÉRDÉSEK

Számos támadás éri a Zoom adatkezelési gyakorlatát. Lássuk be nem minden ok nélkül. A szolgáltató rengeteg adatot gyűjt a felhasználókról (a profilban megadott személyes adatokat, a csatlakozáskor használt eszköz adatait, bejelentkezéshez használt profilok adatait stb.) és nem fél őket használni. A sok kezdeti probléma ellenére most az látszik, hogy a legnagyobb felháborodást kiváltó hibákat a szolgáltató igyekszik javítani: az olyan problémás funkciókat, mint a *LinkedIn Sales Navigator* (az előfizetőknek automatikusan feldobta a részvevők LinkedIn profilját), vagy az *Attendee attention tracking* (jelezte a szervezőnek, ha valamelyik résztvevő hosszabb ideig más ablakot használ a beszélgetés ideje alatt) levették a felületről; több hibát javítottak; a *Company Directory* funkciónál (ez elvileg azt teszi lehetővé, hogy a felhasználók láthassák a munkatársaikat) a bejelentések alapján szűrik a domaineket; a beszélgetés rögzítéséről üzenet jelenik meg stb. Emellett az adatvédelmi tájékoztatóból is kivették a legdurvább részeket így a jelenlegi változat szerint a szolgáltatás használatával kapcsolatos adatokat nem, csak az olyan „marketing weblapok” látogatásával kapcsolatos adatokat használják reklámcélokra, mint a zoom.us.

Azzal azért legyünk tisztában, hogy „nincs ingyen ebéd”. Amikor valaki ingyenesnek mondott programot használ, akkor azért valójában az adataival fizet. Mit tehetünk?

Duna Tower , 1138 Budapest, Népfürdő u. 22.
t: +36 1 2704-835, f: +36 1 2704-329, e: info@kancellar.hu, w: kancellar.hu

- Regisztrációkor, illetve a profilunkban csak a legfontosabb, a kapcsolattartáshoz nélkülözhetetlen adatokat adjuk meg;
- Ellenőrizzük az adatvédelmi illetve a sütik kezelésére vonatkozó beállításokat és állítsuk be a számunkra még elfogadható, leginkább korlátozó opciókat. Ha nincs ilyen ne használjuk a szolgáltatást.
- Olvassuk el az adatvédelmi tájékoztatót mielőtt elfogadjuk. Ha olyan dolgokat ír, ami nekünk nem fér bele, akkor ne használjuk a szolgáltatást.

KONFERENCIAHÍVÁSOK TITKOSÍTÁSA

A Zoom korábban több helyen (köztük a magán a felületen is) azt állította, hogy a kapcsolat a végpontok között titkosított (a szolgáltatás képes end-to-end encryptiont megvalósítani), ami komoly fegyvertény, hiszen a legtöbb hasonló szolgáltatás ezt nem tudja. Kiderült azonban, hogy ez ebbe a formában nem igaz. Azóta közzétettek egy pontosítást, amiben elnézést kérnek a „félreérthető” megfogalmazásért és leírják, hogy valójában mit értenek a kapcsolat titkosítása alatt. Nem belemenve a részletekbe nagyjából azt, hogy általában titkosított a kapcsolat, de bizonyos esetekben (például a hívás rögzítésekor, vagy ha valaki vonalas telefonról kapcsolódik be a konferenciahívásba) a szolgáltatónak szerver oldalon fel kell oldania a titkosítást. Azaz a kommunikáció a Zoom szervere és a beszélgetés résztvevői között ugyan titkosítva történik, azonban ezt a titkosítást a szerver végződteti – tehát a szerver üzemeltetői (ez esetben a Zoom) minden meeting teljes tartalmához hozzáférhet. Ezt valahogy úgy lehet értelmezni, hogy a világ többi része azt gondolja a végpontok közötti titkosításról, hogy azt a végpontokon kívül más nem tudja dekódolni (még a szolgáltató sem), mert nincs meg a dekódoláshoz szükséges kulcs, viszont a Zoom ezt úgy értelmezte, hogy ugyan ők vissza tudnák fejteni a titkosítást, (mert a kulcs megvan nekik is) de általában nem akarják. Emellett az is kiderült, hogy a titkosításhoz olyan elavult kriptográfiai megoldást használnak (a ’80-as évek beli ECB-t), amit a szakma közel sem tekint biztonságosnak.

A jó hír az, hogy a Zoom dolgozik egy olyan megoldáson, ahol a titkosító kulcsokat nem a szolgáltató generálja, kezeli, tárolja, hanem a felhasználók maguk tehetik ezt meg saját üzemeltetésű környezetben.

Addig is csak annyira bizalmas információkat osszunk meg a konferenciabeszélgetéseken, amennyire a szolgáltatóban megbízunk. Boris Johnson egy Twitter bejegyzése alapján például a kabinetüléseket tartja itt…

Duna Tower , 1138 Budapest, Népfürdő u. 22.
t: +36 1 2704-835, f: +36 1 2704-329, e: info@kancellar.hu, w: kancellar.hu

NYILVÁNOSSÁGRA KERÜLT TARTALMAK

Sok ezer rögzített Zoom hívást lehet találni a videómegosztókon és mindenféle felhő alapú fájlmegosztó, -tároló szolgáltatásokon, amelyek döntő többségét biztos nem a nagy nyilvánosságnak szánták a felvételeken szereplők. Ezek eredete nem ismert, nem lehet tudni, hogy esetleg a szolgáltatótól kerültek ki, vagy a felhasználók hanyagsága, figyelmetlensége miatt érhetők el a publikus neten, bár az utóbbi egyáltalán nem lenne meglepő. A The Washnington Post több ilyen nyilvánosan elérhető felvételen szereplő személyt azonosított és megszólaltatott, akik elmondták, hogy fogalmuk sem volt róla, hogy a felvételek nyilvánosan elérhetők és a beszélgetés témája, tartalma (pl. intimitása) és a megszólalók egyértelmű azonosíthatósága miatt ez igen kellemetlenül érinti, felháborítja a beszélgetések résztvevőit.

Az ilyen helyzeteket úgy kerülhetjük el a legkönnyebben, ha egyáltalán nem rögzítjük a konferenciahívásokat, különösen azért is, mert a beszélgetések rögzítése rengeteg, a résztvevők személyiségi jogainak védelmével, személyes adatainak kezelésével kapcsolatos adatvédelmi kérdést is felvet.

Ha mégis elkerülhetetlen a beszélgetés rögzítése, akkor ezt csak a résztvevők tudtával és egyértelmű hozzájárulásával tegyük meg és fokozottan figyeljünk a felvétel hozzáférés-védelmére (ha kell kétszer is ellenőrizzük, hogy olyan helyre mentettük-e le, ami nincs nyilvánosan megosztva és csak azok rendelkeznek hozzáférési joggal, akiknek erre feltétlenül szüksége van). Ha már nincs szükség a felvételre töröljük azt.

Azzal azért legyünk tisztában, hogy egy videóhívásról akár a tudtunk nélkül is készülhet felvétel, ezért csak olyan dolgokat tegyünk, csak olyan dolgokat mondjunk, csak olyan dolgokat mutassunk meg, ami miatt később nem kell kellemetlenül éreznünk magunkat.

KONKLÚZIÓ

Kell-e sátánt kiáltani? Közellenségnek kell-e bélyegezni a Zoomot? Valószínűleg nem. Meg kell-e feltétel nélkül bízni a szolgáltatásban és itt kell-e megosztani a legféltettebb titkainkat? Egészen biztosan nem.

Kezeljük a Zoomot annak, ami! Tekintsünk rá egy jól használható, de biztonsági és adatvédelmi szempontból még gyermekcipőben járó szolgáltatásként és bízzunk benne, hogy a szolgáltató körül támadt vihar hozzájárul a biztonsági hiányosságok feltárásához, mielőbbi javításához.

Használjuk tudatosan, arra amire való, a fenti problémák, gyengeségek és a videokonferenciák sajátosságaiból adódó fenyegetések tiszteletben tartásával. Ha betartjuk a legalapvetőbb óvintézkedéseket, akkor egy baráti beszélgetés, egy tanóra, egy edzés, vagy egy egyszerű üzleti beszélgetés lefolytatására egészen biztosan alkalmas, de a cégünk stratégiai fontosságú titkait tartalmazó szerződéseket nem biztos, hogy itt célszerű átküldeni.

Duna Tower , 1138 Budapest, Népfürdő u. 22.
t: +36 1 2704-835, f: +36 1 2704-329, e: info@kancellar.hu, w: kancellar.hu

HASZNOS CIKKEK A SZOLGÁLTATÓ OLDALÁRÓL:

- A Message to Our Users
- Best Practices for Securing Your Virtual Classroom
- How to Keep Uninvited Guests Out of Your Zoom Event
- The Complete Guide to a Secure Zoom Experience
- The Facts Around Zoom and Encryption for Meetings/Webinars
- Response to Research From University of Toronto's Citizen Lab

KAPCSOLÓDÓ CIKKEK, FORRÁSOK:

https://citizenlab.ca/2020/04/move-fast-roll-your-own-crypto-a-quick-look-at-the-confidentiality-of-zoom-meetings/

https://research.checkpoint.com/2020/zoom-zoom-we-are-watching-you/

https://blog.checkpoint.com/2020/03/30/covid-19-impact-cyber-criminals-target-zoom-domains/

https://blog.cryptographyengineering.com/2020/04/03/does-zoom-use-end-to-end-encryption/

https://theintercept.com/2020/03/31/zoom-meeting-encryption/

https://thehackernews.com/2019/07/webcam-hacking-video-conferencing.html

https://thehackernews.com/2020/04/zoom-cybersecurity-hacking.html

https://thehackernews.com/2020/04/zoom-windows-password.html

https://techcrunch.com/2020/04/03/zoom-calls-routed-china

https://techcrunch.com/2020/04/01/zoom-doom/

https://techcrunch.com/2020/03/31/zoom-at-your-own-risk/

https://www.schneier.com/blog/archives/2020/04/security_and_pr_1.html

https://krebsonsecurity.com/2020/04/war-dialing-tool-exposes-zooms-password-problems/

https://www.insidehighered.com/news/2020/04/03/zoombombing-isn%E2%80%99t-going-away-and-it-could-get-worse

https://www.bleepingcomputer.com/news/security/zoom-lets-attackers-steal-windows-credentials-run-programs-via-unc-links/

https://www.theregister.co.uk/2020/04/01/zoom_spotlight/

https://blogs.harvard.edu/doc/2020/03/27/zoom/

https://blogs.harvard.edu/doc/2020/03/28/more-zoom/

https://blogs.harvard.edu/doc/2020/03/29/helping-zoom/

https://blogs.harvard.edu/doc/2020/03/30/zooms-new-privacy-policy/

https://objective-see.com/blog/blog_0x56.html

https://www.theguardian.com/technology/2020/apr/02/zoom-technology-security-coronavirus-video-conferencing

https://www.theguardian.com/technology/2020/apr/02/zoom-says-engineers-will-focus-on-security-and-safety-issues

https://www.nytimes.com/2020/04/02/technology/zoom-linkedin-data.html

https://www.washingtonpost.com/technology/2020/04/03/thousands-zoom-video-calls-left-exposed-open-web/

Duna Tower , 1138 Budapest, Népfürdő u. 22.
t: +36 1 2704-835, f: +36 1 2704-329, e: info@kancellar.hu, w: kancellar.hu